TITLE:

# ルジャンドルによる平方剰余相互法則の証明とその変遷 (数学史の研究)

AUTHOR(S):

高瀬, 正仁

CITATION:

高瀬, 正仁. ルジャンドルによる平方剰余相互法則の証明とその変遷 (数学史の研究). 数理解析研究所講究録 2003, 1317: 10-20

ISSUE DATE:

2003-05

URL:

http://hdl.handle.net/2433/42999

RIGHT:

京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

数理解析研究所講究録 1317 巻 2003 年 10-20



# ルジャンドルによる平方剰余相互法則の証明とその変遷

九州大学大学院数理学研究院　高瀬正仁(Masahito Takase)

Graduate School of Mathematics

Kyushu University

## はじめに

平方剰余相互法則の第一発見者はだれかという問題をめぐり，ガウスとルジャンドルの間に少なからぬ軋轢（あつれき）があったことはよく知られているが，クロネッカーの精密な考証「相互法則の歴史について」（1875年，クロネッカー全集2，3〜10頁）によれば，この法則の最初の発見者はガウスでもルジャンドルでもなくオイラーである．クロネッカーの考証は正確で，オイラーはすでに1783年（オイラーの没年でもある）の論文

「素数による平方数の割り算に関するさまざまな観察」．オイラー全集Ⅰ−3，497〜512頁．この論文は著作『解析小品集』第一巻（64〜84頁）に収録された．

において，後年のガウスと完全に同等の表現様式をもって平方剰余相互法則を記述している．ただし証明が試みられた痕跡はみられない．

平方剰余相互法則の証明を試みた最初の人物は（ガウスではなくて）ルジャンドルである．ルジャンドルは1785年の論文「不定解析研究」において，オイラーやガウスとは異なる形で平方剰余相互法則を記述し，証明を与えた．これが「ルジャンドルによる第一証明」である．後年のルジャンドルは著作『数論の試み』（1798年）にも証明が記載された．この書物は第二版（1808年），第三版（1830年）と二度にわたって改訂版が刊行され，どの版にも，平方剰余相互法則の（改訂された）証明が収録されている．1798年の『数論の試み』の初版は未見だが，第二版，第三版の記述から推して，この版には1785年の論文「不定解析研究」の証明と同じ証明が採用されたと見てよいと思われる．そこでそれを「第一証明」と呼ぶことにしたいと思う．ただしこの第一証明には論理上の不備があり，正しい証明とみなすことはで

きなかった.

ルジャンドルの第一証明の欠陥の所在地を正しく指摘したのはガウスであった. ガウスは，ルジャンドルの著作『数論の試み』から三年後に刊行された著作 "Disquisitiones Arithemeticae"（1801年. 邦訳『ガウス整数論』朝倉書店，1995年）においてルジャンドルの証明に精密な検討を加え，「正しい証明とはみなされえない理由」を詳述するとともに，相異なる原理に基づく二通りの正確な証明を与えた. このような経緯を振り返ると，

平方剰余相互法則を最初に記述したのはオイラー，

最初に証明を試みたのはルジャンドル，

最初に正しい証明に成功したのはガウス

である.

ガウスの批判を受けて，ルジャンドルは第一証明の改良の試みを継続し，長い年月にわたり，『数論の試み』の改訂版の中で公表した. そこで1808年に刊行された『数論の試み』第二版所収の証明を「第二証明」，1830年の第三版『数論』（書名から「試み」という語句が削除された）所収の証明を「第三証明」と呼ぶことにしたいと思う. これらの二通りの証明は依然として未完成であり，そのために「ルジャンドルは平方剰余相互法則の証明には成功しなかった」という認識が一般に流布される結果になった.

だが，他方，ルジャンドルは『数論の試み』第三版『数論』において，平方剰余相互法則とは無縁の場所でゆくりなく正しい証明に遭遇した（『数論』巻2，56頁）. すなわち**ルジャンドルは平方剰余相互法則の証明に成功したと言える**のである. これはルジャンドルにとっても思い掛けない出来事だったようであり，数論の歴史叙述の中で一般に指摘されることのない事実と思う. そこで本稿では，（1）ルジャンドルによる三通りの証明を概観し，（2）ルジャンドルの第一証明に加えられたガウスの批判を検討し，最後に，（3）ルジャンドルが「正しい証明」に遭遇した様子を観察したいと思う.

# Ⅰ．　ルジャンドルの第二証明と第三証明

ルジャンドルに対して第一証明の改訂に向かう契機を与えたのは，第一証明に寄せられたガウスの批判であった．次に引くのは，ルジャンドル自身が『数論の試み』第二版「緒言」において語っている言葉である．

**ルジャンドル『数論の試み』第二版「緒言」より**

この著作［ガウス『整数論』］は1801年にライプチヒで刊行されたが，これによりこの書物の著者は，一気にもっとも名高い解析学者たちの階層に列せられたのである．この書物には，1798年に出版された『数論の試み』において取り扱われた事柄に類似の事柄がたくさん含まれている．わけても**そこには，すでに引き合いに出された相互法則の，直接的な，しかもきわめて巧妙な一つの証明が出ている**．その証明は，はるかに広い範囲に広がる叙述と併せて，この第二版に載せるつもりであった．ところが著者［ルジャンドル］はその後，**ずっと簡単で，しかもはるかに優美な証明をうまく見つけた**．そこでそちらの証明を選定して，それを第四部§Ⅶで記述した．

ここに言われている「ずっと簡単で，しかもはるかに優美な証明」というのが本稿でいう第二証明であり，『数論の試み』第二版に収録された．『数論の試み』第三版に移ると第二証明になお残されていた不備を補おうとして，「改訂された第二証明」が現われた．それが第三証明である．

そこで初めに平方剰余相互法則に対するルジャンドルの第二証明と第三証明を概観したいと思う．ルジャンドルにならって，奇素数の全体を$4x+1$と$4x+3$という二通りの形状に応じて二分する．一般に前者の素数を$A, a, \alpha$という文字で表わし，後者の素数は$B, b, \beta$という文字で表わすことにする．平方剰余相互法則は，奇素数$m$，$n$の形状とルジャンドル記号$\left(\frac{n}{m}\right)$の符号に応じて，下記のような八通りの場合に分けられる．

Ⅰ．　$\left(\frac{a}{b}\right)=-1$ なら $\left(\frac{b}{a}\right)=-1$．

Ⅱ．　$\left(\frac{b}{a}\right)=+1$ なら $\left(\frac{a}{b}\right)=+1$．

III. $\left(\frac{B}{b}\right)=+1$ なら $\left(\frac{b}{B}\right)=-1$.

IV. $\left(\frac{B}{b}\right)=-1$ なら $\left(\frac{b}{B}\right)=+1$.

V. $\left(\frac{a}{A}\right)=+1$ なら $\left(\frac{A}{a}\right)=+1$.

VI. $\left(\frac{a}{A}\right)=-1$ なら $\left(\frac{A}{a}\right)=-1$.

VII. $\left(\frac{a}{b}\right)=+1$ なら $\left(\frac{b}{a}\right)=+1$.

VIII. $\left(\frac{b}{a}\right)=-1$ なら $\left(\frac{a}{b}\right)=-1$.

場合Ⅰと場合IIの証明は正しい．場合IIIと場合IVの証明も正しい．場合Ⅴと場合VI，および場合VIIと場合VIIIの証明は，

**与えられた素数 $a$ に対し，条件 $\left(\frac{a}{\beta}\right)=-1$ をみたす素数 $\beta$ が存在すること**

を仮定すれば正しい．この間の事情を語るルジャンドルの言葉を聞こう．

**『数論の試み』第三版『数論』， 235～237頁より**

初めの四通りの場合は完全に証明され，これ以上望むべきことは何も残されていないと言ってよい．**他の四通りの場合では，ある一つの事柄が仮定されている**．それは，$4n+1$ という形の数 $a$ が与えられたとき，式 $x^2+a$ を割り切るような $4n+3$ 型の素数 $\beta$，したがって $\left(\frac{a}{\beta}\right)=-1$ となるような数 $\beta$ をつねに見つけることができる，ということである．

この補助的素数の存在は，$a$ が $8n+5$ という形のときにはすぐに証明される．実際，$x=1$ と置くと式 $x^2+a$ は $1+a$ となるが，これは $8n+6$ 型である．それゆえこれは $4n+3$ 型の数で割り切れ，したがって同じく $4n+3$ 型のある素数で割り切れることになる．その素数を，$\beta$ として採れるのである．

$a$ が $8n+1$ という形のときには，この形状は，3の倍数を基準にして考えると，$24n+1$ 型と $24n+17$ 型という二通りの形状に分かれることがわかる．このうち後者の形状に関して言うと，ここでもまた $x=1$ と置けば十分である．そのようにすると $x^2+a$ は $24n+18$ という形になるが，これは3で割り切れるか

ら $\beta=3$ と採ることができて，条件 $\left(\frac{a}{\beta}\right)=-1$ は $24n+17$ 型のあらゆる素数 $a$ に対してみたされるのである．

それゆえなお示さなければならないのは，1は除くことにして，$24n+1$ という形のどの素数 $a$ に対しても，$4n+3$ 型であってしかも $z^2+a$ の約数でもあるような素数 $\beta$，あるいは同じことになるが，条件 $\left(\frac{a}{\beta}\right)=-1$ をみたす素数 $\beta$ をつねに見つけることができるという事実である．

まず初めに簡単な代入によりたやすく示されるように，6通りの形状

$$a=168x+17,\ 41,\ 73,\ 89,\ 97,\ 145 \quad \textbf{(註1)}$$

のどれかに包摂されるどの素数 $24n+1$ にも，各々に対応して値

$$z=2,\ 1,\ 2,\ 3,\ 1,\ 3$$

を取れば式 $z^2+a$ は7で割り切れるという性質が備わっている．したがってこれらの形状に包摂されるどの素数に対しても，値 $\beta=7$ は条件 $\left(\frac{a}{\beta}\right)=-1$ をみたす．

同様に，10通りの形状

$$a=264x+17,\ 41,\ 65,\ 73,\ 145,\ 161,\ 193,\ 217,\ 233,\ 241 \quad \textbf{(註2)}$$

のうちのどれかに包摂されるどの素数 $24n+1$ にも，各々に対応して値

$$z=4,\ 5,\ 1,\ 2,\ 3,\ 2,\ 4,\ 5,\ 3,\ 1$$

を取れば式 $z^2+a$ は11で割り切れるという性質が備わっている．こうしてこのようなどの素数 $a$ に対しても，$\beta=11$ を採れば条件 $\left(\frac{a}{\beta}\right)=-1$ がみたされる．

限界1009までの素数 $24n+1$ は15個，存在する．すなわち，

$$73,\ 97,\ 193,\ 241,\ 313,\ 337,\ 409,\ 433,$$
$$457,\ 577,\ 601,\ 673,\ 769,\ 937,\ 1009$$

である．これらの15個の数のうち，10個の数 $a$ は条件 $\left(\frac{a}{7}\right)=-1$ をみたす．それらは，

$$a=73,\ 97,\ 241,\ 313,\ 409,\ 433,\ 577,$$
$$601,\ 769,\ 937$$

である．他の5個の数 $a$ は条件 $\left(\frac{a}{11}\right)=-1$ をみたす．それらは，

$$a=193,\ 337,\ 457,\ 673,\ 1009$$

である（**註3**）．それゆえわれわれが仮定した事柄は限界 $a=1009$ までは確認

された．同時に，上に挙げたいくつかの式に包摂されている無限に多くの素数に対してもまた確かめられた．だが肝心なのは，1は除くことにして，$8n+1$という形のどの素数$a$に対しても，われわれの仮定は一般的に正しいことを示すことである．

（註1）　三つの形状 $168x+17$，41，89 は $24n+1$ 型ではない．

（註2）　五通りの形状 $264x+17$，41，65，161，193，233 は $24n+1$ 型ではない．

（註3）　二条件 $\left(\frac{a}{7}\right)=-1$，$\left(\frac{a}{11}\right)=-1$ を同時にみたす数も存在する．たとえば73はそのような数である．

ここまでは『数論の試み』第三版『数論』の記述だが，第二版ではほぼ同じ内容がもう少し大雑把に書かれている．これが**第二証明**である．

この第二証明はこれだけではまだ不十分で，ルジャンドル自身が明記しているように，$a$が$8n+1$型の素数の場合に対する「補助的素数$\beta$の存在証明」，すなわち

「1は除くことにして，$8n+1$という形のどの素数$a$に対しても，われわれの仮定は一般的に正しいこと」

を証明しなければならないが，第三版に移ると記述が増補されて，この残る論点の証明が記述された．これを第二証明と合わせると，その全体が**第三証明**を構成するのである．

## Ⅱ．　ルジャンドルの第一証明

ルジャンドルによる平方剰余相互法則の**第一証明**が現われたのは，1785年の論文「不定解析研究」においてである．この証明では，平方剰余相互法則は次のような8個の定理に分けられている．

Ⅰ．　$\left(\frac{b}{a}\right)=+1$ なら $\left(\frac{a}{b}\right)=+1$．

Ⅱ．　$\left(\frac{a}{b}\right)=-1$ なら $\left(\frac{b}{a}\right)=-1$．

III. $\left(\frac{a}{A}\right)=+1$ なら $\left(\frac{A}{a}\right)=+1$.

IV. $\left(\frac{a}{A}\right)=-1$ なら $\left(\frac{A}{a}\right)=-1$.

V. $\left(\frac{a}{b}\right)=+1$ なら $\left(\frac{b}{a}\right)=+1$.

VI. $\left(\frac{b}{a}\right)=-1$ なら $\left(\frac{a}{b}\right)=-1$.

VII. $\left(\frac{b}{B}\right)=+1$ なら $\left(\frac{B}{b}\right)=-1$.

VIII. $\left(\frac{b}{B}\right)=-1$ なら $\left(\frac{B}{b}\right)=+1$.

この区分けは第二証明における区分けとは一致しない．対応関係は次の通りである．

第一証明　I　II　III　IV　V　VI　VII　VIII

第二証明　II　I　V　VI　VII　VIII　III　IV

IとII，IIIとIV，VとVIはそれぞれ一方が他方の対偶になっているから，これらの6個の定理I～VIのうち，実際に証明の対象になる定理は3個である．それらにVIIとVIIIを合わせて，実質的には全部で5個の定理が提示されていることになる．ガウスは『整数論』においてルジャンドルの証明を批判する際，このように五通りの場合に区分けして相互法則を再現した．

第一証明では三種類の補助的素数の存在が仮定されている．

**第一種補助的素数**

相異なる奇素数 $p$, $q$ に対し，条件 $\left(\frac{a}{p}\right)=-1$, $\left(\frac{a}{q}\right)=-1$ をみたす $4n+1$ 型の素数 $a$．（定理V，VI，VII）

**第二種補助的素数**

$4n+1$ 型の素数 $A$ に対し，条件 $\left(\frac{A}{b}\right)=-1$ をみたす $4n+3$ 型の素数 $b$．（定理III, IV．第二の方法）

**第三種補助的素数**

相異なる二つの$4n+1$型の素数$a$, $A$に対し，条件$\left(\frac{b}{a}\right)=+1$, $\left(\frac{A}{b}\right)=-1$をみたす．
$4n+3$型の素数$b$．（定理III, IV．第一の方法）

これらの三種類の補助的素数のうち，第二証明で要請されている素数，すなわち「与えられた素数$a$に対し，条件$\left(\frac{a}{\beta}\right)=-1$をみたす素数$\beta$」に相当するのは第二種補助的素数である．第一種と第二種の補助的素数は第二証明にはもう使われないから，「存在証明なしに使われる補助的素数」の種類は減少し，証明全体の構成は非常に見通しのよいものになった．この点において，第二証明は第一証明に比して大幅に改良されたと言えるように思う．

# Ⅲ．　第一証明に対するガウスの批判

## 1．　1785年の論文「不定解析研究」における証明に対する批判

ガウスは『整数論』第5章の末尾の2節．第296条と第297条において，ルジャンドルの第一証明に批判を加えた．これらの二条には，

「ルジャンドル氏が基本定理を取り扱った方法について」

という小見出しがついている．ガウスはルジャンドルの第一証明を五通りの場合Ⅰ～Ⅴに区分けして再現したが，これをルジャンドルの区分けと照合すると，対応関係は次の通りである．

| | | | | | |
|---|---|---|---|---|---|
| ガウスにより再現された第一証明 | Ⅰ | Ⅱ | Ⅲ | Ⅳ | Ⅴ |
| ルジャンドルの原証明 | Ⅶ | Ⅰ, Ⅱ | Ⅲ, Ⅳ | Ⅴ, Ⅵ | Ⅷ |

ガウスの批判は「三種類の補助的素数の存在が確立されていない」という点に向けられた．

(a)　第一種補助的素数について

この素数の存在証明は「アリトメチカ的数列の素数定理」（「初項と公差が互い

に素なアリトメチカ的数列の中には無限に多くの素数が存在する」ということを主張する定理）に帰着される．ガウスはこの事実を指摘した．ルジャンドルはこの論点には気づいていなかったと思われる．ただしルジャンドルは「アリトメチカ的数列の素数定理」を記述して証明を試みた最初の人物である．

(b)　第二種補助的素数について

これについてガウスは次のように語り，そのような素数の存在に疑念を表明した．

> ところがもうひとつの仮定（III，第二の方法），すなわちある$4n+3$型の素数$r$で，もうひとつの与えられた$4n+1$型素数$p$がその非剰余になるという性質を備えているものが存在するという仮定については，ルジャンドルは何も所見を添えなかった．（ガウス全集1，357頁）

(c)　第三種補助的素数について

この種の素数についてもガウスの見方は明快である．がうすはただ次のように言うのみである．

> 最後に，場合IIIの第一の方法における仮定はいっそういわれのないものなのであるから，それについてここで何事かを言い添える必要はない．（ガウス全集1，357頁）

## 2.　『数論の試み』第一版に見られる証明に対する批判

ガウスの『整数論』の巻末には「補記」がついていて，全部で五つの記事があるが，そのうちの二つまでがルジャンドルの著作『数論の試み』第一版に関するものである．一つは「第151, 296, 297条に寄せる補記」で，ルジャンドルによる平方剰余相互法則の証明をめぐる所見である．これを読むと，『数論の試み』第一版に出ている証明には依然として第一種補助的素数と第二種補助的素数の存在が仮定されていると推測される．ガウスの補記には第三種補助的素数への言及はないが，このような状勢から推して，『数論の試み』第一版に出ている証明は1785年の論文「不定解析研究」の証明（第一証明）と同一と見てよいように思う．

平方剰余相互法則に対するルジャンドルの証明への批判としてしばしば繰り返されるのは，「アリトメチカ的数列の素数定理が証明されないままで使われている」という指摘である．このような批判の様式には次に挙げるような問題があり，不適切と思う．すなわち，

(1)　ルジャンドルは第一補助的素数の存在証明に「アリトメチカ的数列の素数定理」が必要であることを認識していたわけではない．この認識はガウスが指摘した数学的事実である．ルジャンドル自身は補助的素数の存在を明白と考えていたようで，存在証明が必要という自覚は欠けていたように思う．

(2)　ルジャンドルの第一証明では，第一補助的素数のほかに他の二種類の補助的素数の存在が仮定されていた．第一証明への批判としては（ガウスがそうしたように）この論点を指摘しなければ不十分であり，しかもこのほうがいっそう深刻である．

## Ⅳ．　第一証明の改良の試み

ルジャンドルはガウスの批判を受けて第一証明の改良を試みて，第二，第三の証明を提案した．第二証明では第一種補助的素数と第三種補助的素数はもう使われていないから，ガウスの三つの批判のうち，二つまでは回避された．特に，「アリトメチカ的数列の素数定理」はもう不要である．しかし第二種補助的素数の存在は依然として仮定されている．

第三証明に移り，ルジャンドルは第二種補助的素数の存在証明を試みたが，不完全なままに終わった．『数論の試み』第二版には，ガウスによる第三証明（1808年1月．初等的証明）が収録され，第三版にも受け継がれた．第三版ではさらにヤコビによる証明（円周等分の理論に基づく証明）も紹介された．

## Ⅴ．　第二種補助的素数の存在証明

『数論の試み』第三版『数論』の第四部「さまざまな方法と研究」の第6節「§ VI」

「式 $t^2+au^2$，$a$ は素数 $8n+1$，の二次因子に関する一性質の証明」

という標題がつけられている．第四部の標題から見て取れるように，ここではもう相互法則は主題ではありえない．ところがここに至ってルジャンドルはたまたま第二種補助的素数の存在証明に遭遇した．第四部，第6節，第VI章に出ている第八番目の命題は，

**命題 VIII**　式 $t^2+au^2$，$a$ は素数 $8n+1$，の二次因子 $4n+1$ の個数はつねに，二次因子 $4n+3$ の個数より1だけ大きい．　（『数論』巻2，55頁）

というものだが，第VI章の末尾に次のような「註記」がついている．

**註記**　われわれが取り扱ったばかりの場合において，式 $t^2+au^2$ はつねに三つの二次因子をもつ．すなわち因子　$y^2+2yz+(a+1)z^2$　とその共役因子 $2y^2+2yz+\frac{1}{2}(a+1)z^2$，それに特異因子 $2fy^2+2gyz+fz^2$ をもつが，この特異因子は，$a=1$ という排除される場合においてのみ，先行する二つの因子と一致する．これより明らかになるように，つねに少なくともひとつの二次因子 $4n+3$ が存在する．**これは，第171条でなされた仮定，すなわち相互法則の証明が依拠する仮定を正当化している**．　（『数論』巻2，56頁）

こうしてルジャンドルは第二種補助的素数の存在証明を獲得したが，これはルジャンドル自身の思惑をも越えて，真に偶然性にみたされた出来事であった．それでもこれでルジャンドルの独自の証明が完成したことはまちがいなく，**「ルジャンドルは相互法則の証明に失敗した」という通説は書き改められなければならない**であろう．1785年の論文「不定解析研究」の時点から見て，この間，45年という歳月が流れ，ルジャンドルは（日本流に数えて）79歳という高齢に達していた．没年（1833年1月10日）までわずかに3年弱を残すにすぎず，若い日の相互法則は数学者ルジャンドルの生涯を覆う因縁にみちたテーマになったのである．

［平成14年（2002年）10月31日］